Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 10, Issue. 12, December 2021, pg.1 – 13

Access Control Conflicts in Information Technology and Operational Technology

Robert Kemp
Cyber Technology Institute, School of Computer Science and Informatics, De Montfort University, Gateway House, Leicester, LE19BH
Dr Richard Smith
Cyber Technology Institute, School of Computer Science and Informatics, De Montfort University, Gateway House, Leicester, LE19BH

Corresponding Author – Robert Kemp, p2548837@my365.dmu.ac.uk

DOI: 10.47760/ijcsmc.2021.v10i12.001

Abstract: Access controls are a key area for any security program. However, the recommended access controls cannot always be implemented across the entire organisations. This is the case within critical infrastructure organisations that have both Information Technology and Operational Technology assets where many of the controls cannot be implemented on Operational Technology. Also, safety is a key concern for critical infrastructure organisations which is not always the case with many standard commercial organisations. This means the access controls while maintaining security must not impact safety which can occur if considerations are not given to Operational Technology and safety objectives. This paper will provide ways to manage the conflicts and issues that can occur and provide a process to allow critical infrastructure organisations to implement the required controls without impacting safety and security.
Keywords– Access control, Safety, Security, IT, OT

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

1. Introduction

Security standards such as ISO 27002 - Code of practice for information security controls [IO13] and NIST 800-53 Security and Privacy Controls for Federal Information Systems and Organizations [NT13] specify access controls that should be applied to systems. The objective of the controls are to reduce the risk of unauthorised access and the risks that can occur if access is gained.

These controls can often be implemented for Information Technology (IT) assets and many well-known access control models can be used [AC20]. Implementing these access controls on Operational

Technology (OT) is not as easy and often conflicts and issues will arise [CA12], as the control cannot be implemented in the same manner on the OT asset as it was for the IT asset.

Even when the controls can be implemented the implementation may impact safety [RP13]. If that occurs the organisation needs to find a way to reduce the impact on safety and still implement the control or reduce the risk the control was implemented to manage.

An industry that faces these issues is the Critical Infrastructure (CI) industry. Sectors such as power stations and water treatment plants as examples use both IT and OT systems and have a high demand for safety and security. Breaches in CI organisations have taken place and a lack of access controls has been a cause of the breach. A report [DS16] of a cyber-attack at three Ukraine power stations that caused a blackout highlighted weak access controls were one of the reasons the attack was able to take place.

This paper is looking at logical access control and controlling access to data and systems. Physical access control will not be covered, however many of the concepts and details in this section will be of use in the physical control area as well.

1.1. Problem and novelty of solution

The main problems this paper is going to resolve are certain authentication methods may not work with OT [NT15] or for safety reasons they may need to be bypassed.

Well known security principles such as least privilege [LC07] and segregation of duties can conflict with OT configuration and safety concepts.

Another problem is the account management controls such as the use of shared accounts for OT and the impact of password reset processes on safety [RP15].

The deployment of access control via technology such as Microsoft Active Directory (AD) is not possible on all OT devices.

This paper is going to help resolve those problems and provide a contribution in the OT, safety, and access control area by these activities within the paper:

- Permissions Analysis - Analyse the safety and OT conflicts for various security principles related to permissions and show how to maintain compliance to the security principles while resolving the conflicts.
- Account management - Provide alternative methods to handle account management for OT devices while not impacting safety.
- Authentication remediation - Highlight the conflicts around authentication and provide compensating controls.
- New access control model - Introduce a new access control model that can be used for both security and safety access control objectives.

This paper will review current access controls and identify conflicts in IT, OT, safety, and security. It will provide the details required for the CI organisation to implement the access controls in the OT/IT environment and still meet the safety and security goals of the CI organisation.

Research in this area has focused on creating access control models for various different scenarios such as emergency access [SA15], or a time-based model [EM13] for when availability is critical. A paper by [KB13] looked at making access control decisions based off risk which is similar to what this paper is considering when it comes to access control decisions based on safety and security risks and conflicts.

Many standards such as NIST 800-82 Special Publication 800-82 Guide To Industrial Control Systems (ICS) Security [NT15] and NERC CIP-007-6 Cyber Security – Systems Security Management [NC14] describe access controls that should be applied to OT for CI organisations. However, it does not establish conflicts that can occur when trying to apply the controls from a safety perspective or offer alternative controls. This paper will do that and provide the information required to overcome the problems presented here.

The rest of the paper is organized as follows section 2 will assess the differences between safety, security, IT and OT. Section 3 will briefly cover the recommended access controls that should be applied. The conflicts and issues and how to resolve them will be the focus of section 4. Section 5 will present the Safety Based Access Control (S-BAC) model and the final section of the paper section 6 is the conclusion.

2. Differences with safety, security, IT and OT

2.1. Safety and Security

The objective of safety can be to ensure users are free from harm or injury while security is around protecting data and systems using the security triad of Confidentiality, Integrity and Availability (CIA).

Safety systems have in the past been designed to protect against non-malicious circumstances [RP13] while security systems were designed to protect against intentional malicious circumstances [SK15]. There were exceptions to this but overall, that was the approach taken. As the areas converge more and risks begin to impact them both this is becoming less of a difference.

Terminology is an area where they differ [MB06] with terms such as hazard, vulnerability, control, and safeguard having similar meanings but using different terms.

Security tends to focus a lot of the controls it has on external threats such as unauthorised access while safety has controls which are more internally facing such as equipment failure.

A difference that also impacts the way safety and security operates is that they are managed by separate teams [WY14]. The other differences mentioned such as terms and objectives can mean the two teams take a different approach to each area and do not work closely. This can make it more difficult when both areas are converging more and require an efficient way of working together.

As IT, OT, and the components that CI organisations require become more integrated this also brings safety and security closer together as security incidents can now lead to safety incidents [FR12], which is another reason both areas need to be managed in a more integrated manner.

2.2. IT and OT

The introduction section discussed that many of the problems with access control can be the way the controls are applied to IT, will not be possible with OT. This then either results in controls not being implemented or OT devices and the running of the organisation being negatively impacted. For this reason, it is important to describe what each one is and the differences they have as by understanding the differences the CI organisation should be able to better understand how to apply the controls to both.

IT is a term used to cover many different devices such as routers, laptops, servers, and applications. While OT devices interface with physical devices and can include Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) and Programme Logic Controllers (PLC).

They have both been the subject of cyber security attacks in recent years. For example, malware known as Triton compromised a Saudi Arabian petrochemical plant [DF19] and impacted the OT safety systems. Also, an IT application that customers used to book flights with British Airways was compromised [IO20] resulting in customers credit card details being stolen. Although most security

incidents are IT related OT security incidents are increasing [BF19]. These incidents highlight the need for security controls over both sets of technology.

In the past OT and IT were very distinct separate areas of technology but over time they have converged [CA12] and now interact more closely and share similar technologies. This has advantages but also disadvantages as the risks that IT systems faced are now being faced by OT systems [JH15], but as will be described they are not designed to operate in the same way and for that reason cannot always use the same controls in the same manner to manage those risks.

Unlike IT devices, OT devices did not consider security in the design and use of the systems [YC15].

A difference between IT and OT is the lifespan of the technology, OT is expected to have a much longer lifespan it can be over 20 years while IT is usually much shorter such as around 5 years [OL19]. Even though IT systems have a shorter lifespan they have updates applied throughout that time to help them stay secure and resolve vulnerabilities that were not known at the time of release. OT does not apply the same principal on updates to their systems as there is a strong focus on not impacting availability which an update could have. However, security risks can also impact availability, so this difference needs to be overcome.

OT often uses proprietary or less well-known protocols and does not integrate well with other OT or IT devices. Whereas IT uses more open and well-known protocols, and the systems can interact with each other even when they are created by different vendors.

The reliability of OT and IT is important for the organisation, however for OT due to the physical devices they manage it is even more critical than IT [DT18] and so requires a higher standard of reliability with less risk of failure.

This section has shown some key differences in safety and security as well as IT and OT. These differences are the main reasons it can be difficult to apply access controls to both areas within CI organisations. By understanding the differences, it can help resolve the conflicts and issues that can occur when implementing the required access controls.

3. Access Controls

This section will list the main access controls and give a brief description of each in Table 1 - Access Controls. Control areas often overlap and some controls from another area may be needed for the access controls to operate correctly these controls will be highlighted as supporting controls but will not be covered in detail here.

Control	**Description**
Account Management	There needs to be a process to manage the account through its lifecycle this includes creating, maintaining, and decommissioning the account.
Network Controls	Access to devices can also be managed via network controls. Such as restricting to an IP range, or a certain device. This is covered more under network controls and is a supporting control for this section.
Authentication	Users need to confirm their identity before they can gain access to systems and data. Controls such as requiring a password or access tokens can help authenticate the user.
Permissions	Access rights will be different for different users and the permissions need to be managed from adding permissions to key principles such as least privilege being enforced.
Access Reviews	Over time access rights can become out of date and it is important controls are in place to remediate any issues.

Segregation of duties	Users' roles should not allow for them to override processes such as request and approve a change.
Privileged Access	Certain accounts will be privileged accounts and have more permissions than standard accounts. These accounts will require extra controls due to the increased risk.
Control governance	This is a generic term that captures all the governance tasks around the control such as reporting, metrics and creating the process documentation.

Table 1 - Access Controls

This list is just a brief description of each control and each control will have much more details and implementation options that the CI organisation must decide on. For example, the frequency of the access reviews, how are permissions granted and how is remote access managed are a few example decisions. Standards such as PCI DSS, NIST 800-53 and NERC CIP-007-6 can provide further information on the controls if required.

4. Conflicts and Issue Resolution

Section 3. Access Controls described the controls that CI organisations can use. This section will now analyse the conflicts that can occur and provide solutions that can be put in place.

4.1. Account management

Account management is focused on the user and system accounts and how they are managed. It is closely connected with several HR controls.

4.1.1. Shared accounts

All users should be given a unique individual account but for technical and usability reasons a shared account may be required which will be used by many different people. IT and OT devices may require this, and it conflicts with the security control of accountability. Also, for safety reasons a team may need to use a shared account to access devices as well.

Some potential solutions to this issue are that the shared account should only work on that one device and not have access to other devices where individual accounts can be used. The CI organisation should configure the access to be set to local access and not remote access. This will make it easier to track usage as the user will be onsite and be easier to trace. Another control to track who is using the shared account is every time a user logs in with the shared account, they are prompted on the device to enter their network account username and password which only they will know this is then saved and can help track who uses the account. If the device cannot do the above control, a separate document should be used where users enter their details when they use the account. This can be abused, and users can enter the wrong name so spot checks should be done to ensure users are entering the correct name.

If remote access is required, the user will first have to access a system where they authenticate using their individual username and password and then from there use the shared account to access the device. To limit the risk of the shared account, as few permissions as required should be provided and the password should be reset whenever a user leaves or no longer needs to use the shared account to ensure they can no longer access it. Another option is instead of a shared account, the use of a break glass account can be put in place for times when a user needs to access the device but either their account does not work, or they do not have the required permissions

These solutions should allow the CI organisation to maintain compliance to the security standards while allowing safety and the CI organisation to operate.

4.1.2. Password reset

Before a password is reset it needs to be confirmed the user is who they say they are. If a user is unable to prove who they are they will not be able to reset their password. This can cause issues from a safety perspective if access is required urgently.

Some options to resolve this includes asking the user to contact their line manager who should be able to identify them, they can then contact support to confirm the identity of the user. Another control is as HR would have more personal details about the user then support, HR could speak to the user and verify other details to get confirmation it is the correct person. Or if it is an emergency the support team can contact other members of the user's team and request, they carry out the work and explain what has happened.

These options should allow either the user to be confirmed and password reset, or at least other team members can carry out the work if it is urgent.

4.2. Authentication

For increased security remote access can require multi-factor authentication such as the use of a password and hardware token. A conflict for this control could be that many of the OT devices are not able to operate using the multi factor authentication method, they may only be able to use a password as authentication. Also, the safety team could be concerned if they need access and the authentication method fails or, they lose their device they may not be able to access the systems when required. If that is the case the following methods can help.

To allow remote access for these devices but still enforce multi-factor authentication the CI organisation can use a jump host. This device will allow the user to remotely connect using the multi-factor authentication method and then from there they can access the OT device using their username and password. A concern was if the authentication method fails or is lost it can impact access. If the token fails or the user does not have it, a one-time code to bypass the token can be used and generated by support. However, support must ensure the user is who they claim to be first. The methods used earlier for password resets can also be used here.

Multi-factor authentication is a key control especially for users accessing systems remotely and the controls above can help maintain that control and provide solutions for the occasions it causes issues for the CI organisation.

4.3. Permissions

The permissions given to the accounts should follow certain principles and be managed to reduce the security and safety risks that incorrect permissions can create.

4.3.1. Least privilege

Giving the least amount of permissions required is what security standards state, however many OT and safety devices are limited to the permissions they can provide, and it is often full control only. Also, the safety team may not have a requirement to have certain permissions all the time but in some situations, it may be required quickly. However, the permission of need to know would mean they would not have it right away and need to follow the process to get it added.

Some ways to resolve these conflicts and issues are to implement the control of dual control for certain high-risk tasks on the device and require two administrators to confirm the action. For example, opening the spillway gate requires two accounts to confirm before it takes place. Also, increased logging and monitoring can help detect accidental or intentional changes to the device and if captured early the impact can be reduced. Another control if the safety team needs more permissions in an emergency is the use of a special account. The account will be configured with all the required permissions and can be given to the team at short notice. The account will just need to be enabled when required, if the account is enabled an alert is sent to the safety and security teams and they can investigate why it was enabled and ensure it is for a valid reason. There is still a delay following this

process, but it should be shorter than the delay of requesting permissions and gaining approval and having them added to the users account then removed afterwards.

4.3.2. Screen lockout

All accounts can have permissions that are set up to lock the device after 10 minutes of inactivity. However, the safety team has several monitoring devices that they will not use constantly but need to remain unlocked so they can monitor the information and alerts as they appear.

Some options to resolve this are to allow the account to not lock the device and screen but the user account only has read access to the application. They can see all the systems but to make changes they would need to login with a different account which has the screen lockout enabled. Physical security should be increased and limiting who has physical access to the device can reduce the risk of the screen not locking out. Another option if technically possible on the application/device is the system continues to display the alerts in real time on the screen after 10 minutes but when the mouse is moved, or keyboard pressed to carry out an action the user has to enter their password again.

4.4. Segregation of duties

Segregation of duties is not always possible as the CI organisation will have limited users and the safety team will often require users to manage multiple activities during a shift resulting in permissions that go against the segregation of duties control. Also, OT devices may allow one account to manage the device and access logs and that cannot be changed.

Controls that can be put in place to resolve conflicts in segregation of duties are to require the user to use two separate accounts. By segregating the accounts, it can help stop accidental conflicts. The user would have to make a conscious effort to swap accounts and carry out the task. The CI organisation should ensure all activities carried out by the users are logged and monitored this will help detect when the user is abusing their rights, such as approving their own changes. It is often not possible, but more staff could be hired. A compensating control would be training and awareness, it will help users understand the responsibilities they have and what is considered a conflict and should not be done even if the permissions make it possible. If an OT device has a segregation of duties conflict as they are designed to allow one account to carry out all tasks such as generating the logs and being able to delete them. The logs should be sent off the device to a read only Security information and Event Management (SIEM) solution where they can be monitored. A final control is if the OT device is critical another user could shadow the team member carrying out the work.

Segregation of duties has also been a difficult issue to resolve within IT, due to limited resources. So, having the issue with OT and safety is not unique but adds to the usual conflicts organisation's deal with for segregation of duties.

4.5. Control governance

A lot of the controls discussed so far will use a directory service tool such as Microsoft Active Directory (AD). AD makes the processes easier such as resetting passwords and enabling accounts. For OT devices using AD may not be possible and manual methods will be required. Also, as OT devices may have to have the access controls configured per device the support and OT owners will need to work closely together. Issues can occur when different teams share management of the process and when a large part of it is manual compared to the automated processes the rest of the CI organisation use.

To lower the risk of issues arising the CI organisation can implement one or more of the following solutions. Audits and checks should be conducted more often, as it is a manual process configuration errors are more likely for example not setting the right password complexity. The teams should follow the same settings as AD such as password length it will just have to be enforced on each system. Also, to resolve issues in a timely manner support staff who manage accounts on AD, also need a way to manage the accounts on the OT devices. They should be able to connect over the network to the devices to manage access control changes such as password resets. As a backup control support staff

should also be at the location where the devices are so if needed they can carry out the task locally at the device. Access reviews and account management should consider manual accounts and actions required and not just focus on AD. As a lot of the work will be manually done there should be a documented process created, and the asset owners given training on how to follow them. If the asset owners fail to follow the access control processes, then disciplinary action should be taken.

The need for manual processes for OT access control does not mean the controls will be less effective but it can be more time-consuming and require more resources to manage it to the same level as using a directory service like AD.

The controls and activities that have been described in this section are designed to reduce the risks of conflicts or remove the conflicts and allow the CI organisation to still carry out the access controls.

5. Safety Based Access Control (S-BAC) model

The access controls discussed in this paper can be applied using an access control model that has been created called Safety Based Access Control (S-BAC). The model can be used in Role Based Access Control (RBAC) or Attribute Based Access Control (ABAC).

The key requirements of the S-BAC model are:

- It can be applied to all IT and OT systems and other hardware
- Security is enforced by default
- Safety is not compromised by the access control policies
- The model can respond to changes in safety and security

The objective of the requirements is to ensure the access controls can be applied to all applicable assets while not causing safety issues. To do this the S-BAC model will change the access controls as needed depending on the situation. The main components of the S-BAC model are:

- Users (U) – The users are making the access requests.
- Object (O) – The asset that the user requires access to.
- Roles (R) – Users may be placed in roles such as database administrator. If RBAC is being used.
- Attributes (A) – Describes details about the user, object, or permissions. If ABAC is being used.
- Permissions (P) – Privileges the user has such as read access.
- Security Policy (SecP) – This is the set of rules to determine if the requested access should be allowed, given the values of the attributes/roles of the user, object, and permissions. From a security perspective.
- Safety Policy (SafP) – This is the set of rules to determine if the requested access should be allowed, given the values of the attributes/roles of the user, object, and permissions. From a safety perspective.
- Conflict Resolution (CR) – Certain elements of the security policy may conflict with the safety policy and the conflict resolution will resolve those conflicts.
- Security Conditions (SecC) – These conditions will cover the security situation that the access request comes in from. It will be discussed later but the security condition for the request could be during a security breach, normal operations etc.

- Safety Conditions (SafC) - These conditions will cover the safety situation that the access request comes in from. The safety condition for the request could be during an emergency, normal operations etc.

Figure 1 - S-BAC Model shows the components and the way they each interact with each other when an access request is made.

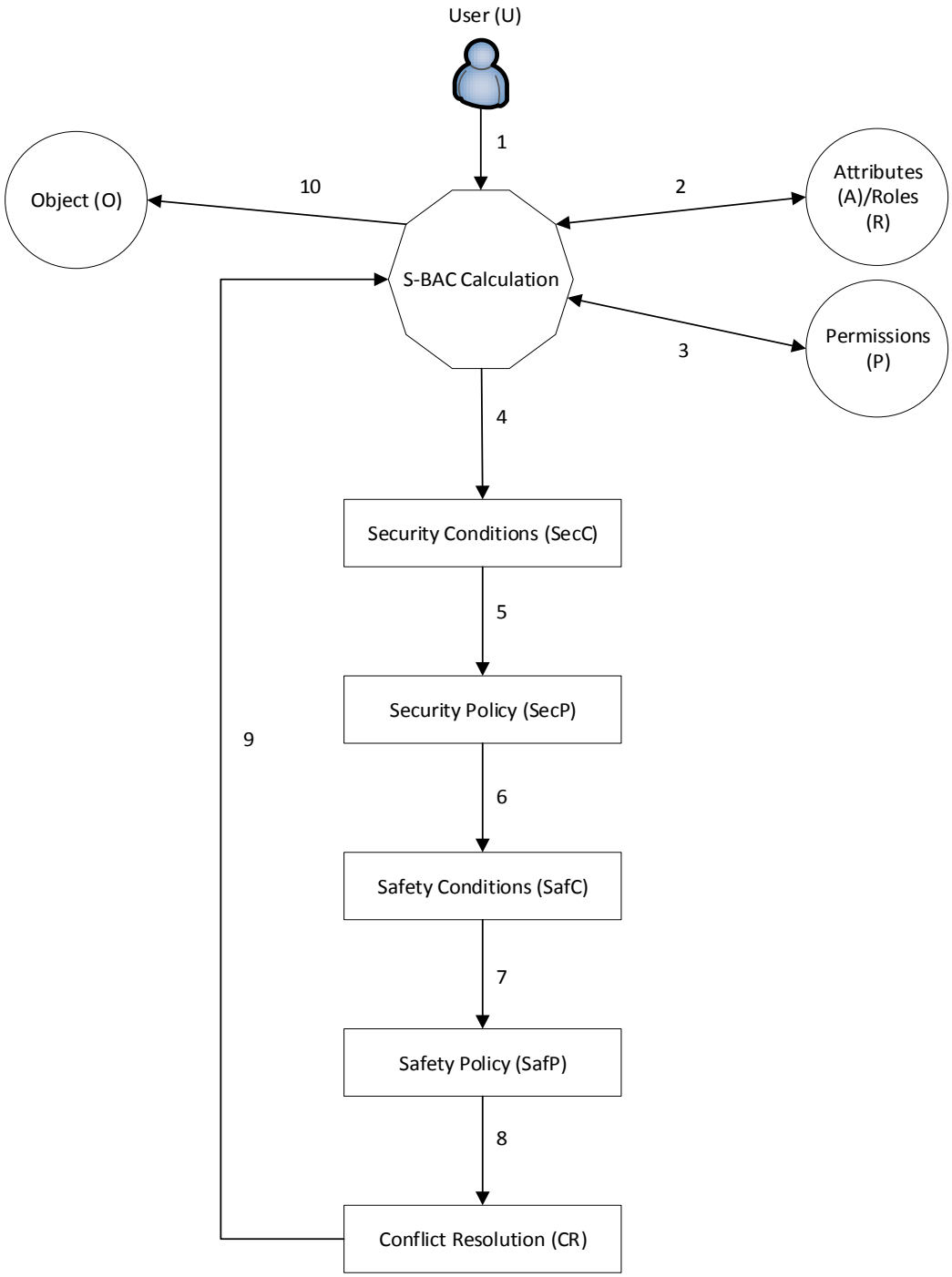

Figure 1 - S-BAC Model

A brief introduction to the steps in the model is given here and for the steps where more detailed information is needed that is given after the steps.

Step 1 – User requests access to an object such as SCADA server, or word document.

Step 2 – S-BAC calculation checks what roles\attributes the user has.

Step 3 – The S-BAC calculation checks the user's permissions to the requested object.

Step 4 – The S-BAC calculation establishes what the current security condition is for the object and organisation.

Step 5 – Once the security conditions has been established, the security policies that are used for that condition are evaluated.

Step 6 – Similar to step 4 but this time it is checking the current safety condition.

Step 7 - Once the safety condition has been established, the safety policies that are used for that conditions are evaluated.

Step 8 – As the security and safety policies have now been selected the S-BAC calculation analyses them both for conflicts between the policies.

Step 9 – The conflict resolution steps are then followed to resolve the conflicts, with the final access control permissions established by the S-BAC calculation.

Step 10 – The user is provided access to the object with the calculated access control rules.

The safety (SafC) and security (SecC) condition components of the model represent the conditions of the object or wider organisation during the user's access request. The reason different conditions are defined is because the required access control policy may change depending on what the safety or security condition is. For example, a different set of security rules would be applied during a security incident condition compared to normal operation. The defined conditions are:

- Normal operation
- Emergency operation
- Security incident
- Safety incident

In Figure 1 - S-BAC Model once the safety and security conditions have been established and the corresponding access control policy has been applied. The conflict resolution component will assess both policies in respect of the subject and object to see if conflicts occur.

For example, the subject is required to use their individual account to access the object (stated in the security policy), but as the condition is a safety incident the subject requires the use of a shared administrator account (stated in the safety policy) these two rules conflict. The conflict resolution component assesses the conflict and performs the required steps which in this case is to allow access to the shared account while the safety condition remains at safety incident. While limiting the shared administrator account access to only the required device and also alerts the security and safety teams of the results so they can be investigated if required.

Resolutions to the conflicts can use the recommend controls in section 4 Conflicts and Issue Resolution while the main controls mentioned in section 3 Access Controls will help create the access control policies.

Deciding on the safety and security conditions can be automated or done manually. The team can use the alerts that come from the assets and use them to help define certain conditions. For example, if an alert comes in that an asset that has been classed as critical and has a high uptime is showing as offline the alert will cause the condition to change to emergency and then the emergency safety and security access control policies will be used. It can also be done manually by the team that manage the access control processes for the organisation. If they became aware of a security incident and have detected unauthorised access on the network, they could set the security condition to security incident while the safety condition could remain at normal operation. The access control policies for security would use the security incident ones while safety remains using the normal operation access control policies. The conflict resolution component may respond differently on the safety and security access control policies depending on the conditions as well. In the previous example due to the security condition of security incident the security policies may override a safety access control rule that is usually allowed under normal conditions.

Controls have to be in place to stop the misusing of the safety and security conditions. One option is to have a time delay before changing conditions this allows the organisation to check if the change is required and is not being done to bypass access controls. The time delay could be 10 minutes and then it automatically changes conditions, or it could be set to not change until approved.

Increased logging and monitoring should take place when conditions change from normal, to detect if malicious actions are occurring due to the change in access control policies. The safety and security conditions should be changed back to normal operation as quickly as possible. If it looks like the issue may go on for a long time the access control team can look to give a few users extra permissions during that period, then change back to normal operation so the rest of the organisation go back to the usual access control policies.

6. Conclusion

This paper has analysed access controls and the impact they can have on OT, safety, and security. The conflicts and issues that can arise were highlighted and remediation activities were created which was the aim of this paper.

This paper has shown that often a control that can be applied to IT, is not technically possible for OT or if it can be applied it can have a potentially negative impact on safety. The paper offered alternative controls that can comply with the aim of the original security control or at least reduce the risk while reducing the impact on safety.

The access control model that was created provides a good base to build on to implement many of the concepts and controls discussed in this paper. It was designed to be customised to suit the organisation and can be changed as required.

If a CI organisation did not implement an access control because it was going to impact safety, they need to consider that there could still be an impact to safety. As although the control was related to security if a security issue arises it could become a safety incident. This is one of the reasons safety and security need to be managed together and ways to implement controls in both areas need to be found rather than looking to avoid controls that negatively impact safety without considering the longer-term impact of that choice.

A future piece of work could be for the S-BAC model to have the algorithms and rules created to allow the model to be used by organisations.

It is likely security and safety requirements will increase in the future thus the occurrences of conflicts will continue to raise. The need to resolve those conflicts while maintaining safety and security will be even more important in the future and the methods used here can be applied to other security areas as needed.

References

[1]. [AC20] R. Ausanka-Crues, Methods for Access Control: Advances and Limitations, 2020

[2]. [BF19] B. Filkins and D. Wylie, SANS 2019 State of OT/ICS Cybersecurity Survey, 2019

[3]. [CA12] C. Alcaraz, F. Gerardo and C. Fernando, Security aspects of SCADA and DCS environments. In Critical Infrastructure Protection, pp. 120-149. Springer Berlin Heidelberg, 2012

[4]. [DF19] D. Franzetti, Oil & Gas Cybersecurity and Process Safety Converge Thanks to TRITON, 2019, Accessed 2020, https://securityboulevard.com/2019/02/oil-gas-cybersecurity-and-process-safety-converge-thanks-to-triton/

[5]. [DS16] United States Department of Homeland Security, ICS Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure, Access 2019, https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01

[6]. [DT18] D. Timpson and E. Moradian, A Methodology to Enhance Industrial Control System Security. Procedia Computer Science. 126. 2117-2126, 2018. 10.1016/j.procs.2018.07.240.

[7]. [EM13] E. Magkos and V. Chrissikopoulos, T-ABAC: An attribute-based access control model for real-time availability in highly dynamic systems. Proceedings - International Symposium on Computers and Communications, 2013. 000143-000148. 10.1109/ISCC.2013.6754936.

[8]. [FR12] F. Reichenbach, J. Endresen, M. Chowdhury and J. Rossebo, A Pragmatic Approach on Combined Safety and Security Risk Analysis, 21012. 239-244. 10.1109/ISSREW.2012.98.

[9]. [IO13] International Organization for Standardization, Information technology — Security techniques — Information security management systems — Requirements, Second edition, 2013.

[10]. [IO20] Information Commissioner's Office, British Airways, 2020, Accessed 2020, https://ico.org.uk/action-weve-taken/enforcement/british-airways/

[11]. [JH15] J. Holcomb, Definitive Guide to Cybersecurity for the Oil & Gas Industry, 2015, Accessed 2020, https://www.ciosummits.com/Online_Assets_Leidos_Definitive_Guide_to_Cyber_for_Oil_and_Gas_eBook.pdf

[12]. [KB13] K. Bijon, R. Krishnan and R. Sandhu, A framework for risk-aware role based access control. 2013 IEEE Conference on Communications and Network Security, CNS 2013. 462-469, 2013. 10.1109/CNS.2013.6682761.

[13]. [LC07] C. Liang and J. Crampton, Inter-domain role mapping and least privilege. Proceedings of ACM Symposium on Access Control Models and Technologies, SACMAT. 157-162, 2007

[14]. [MB06] M. Bartnes, Safety vs. security?, Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management May 14-18, 2006, New Orleans, Louisiana, USA, 2006

[15]. [NC14] North American Electric Reliability Corporation, CIP-007-6 — Cyber Security – Systems Security Management, 2014

[16]. [NT13] National Institute of Standards and Technology, Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, 2013

[17]. [NT15] National Institute of Standards and Technology, Special Publication 800-82 Guide To Industrial Control Systems (ICS) Security, 2015

[18]. [OL19] Owl, Protecting Critical Infrastructure in the DoD Landscape, 2019, Accessed 2020, https://owlcyberdefense.com/wp-content/uploads/2019/06/19-OWL-W013-V1-CI-in-the-DoD-Landscape.pdf

[19]. [RP13] R. Piggin, Process Safety and Cyber Security Convergence: Lessons Identified, But Not Learnt? 2013

[20]. [RP15] R. Piggin and H. Boyes, Safety and security – a story of interdependence 2015

[21].[SA15] S. Alves and M. Fernández, A Framework for the Analysis of Access Control Policies with Emergency Management. Electronic Notes in Theoretical Computer Science, 2015. 312. 10.1016/j.entcs.2015.04.006.

[22].[SK15] S. Kriaa, M. Bouissou, L. Piètre-Cambacedes and Y. Halgand, A Survey of Approaches Combining Safety and Security for Industrial Control Systems. Reliability Engineering [?] System Safety. 2015.

[23].[WY14] W. Young and N. Leveson, Inside Risks An Integrated Approach to Safety and Security Based on Systems Theory. Communications of the ACM. 57. 31-35, 2014 10.1145/2556938.

[24].[YC15] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby and K. Stoddart, A Review of cyber security risk assessment methods for SCADA systems. Computers & Security. 56. pp. 1-27. 2015 10.1016/j.cose.2015.09.009.

